



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/076,066	02/15/2002	Michael Staw	37402.010600	8507
22191	7590	10/05/2005	EXAMINER	
GREENBERG-TRAURIG 1750 TYSONS BOULEVARD, 12TH FLOOR MCLEAN, VA 22102			KLIMACH, PAULA W	
		ART UNIT	PAPER NUMBER	2135
DATE MAILED: 10/05/2005				

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	10/076,066	STAW ET AL.
	Examiner Paula W. Klimach	Art Unit 2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 28 May 2002.
 2a) This action is FINAL. 2b) This action is non-final.
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-23 is/are pending in the application.
 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
 5) Claim(s) _____ is/are allowed.
 6) Claim(s) 1-23 is/are rejected.
 7) Claim(s) _____ is/are objected to.
 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
 10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| | 6) <input type="checkbox"/> Other: _____ |



DETAILED ACTION

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rangedahl (5,790,074) in view of Stallings (Cryptography and network security).

In reference to claims 1 and 22, Rangedahl discloses a system for remotely and automatically verifying the location of an electronic device and authorizing operation of the device if it resides in an allowed geographical location (abstract). Rangedahl discloses a location verification server for receiving a location verification request from a user computer desiring authorization to conduct a transaction with a transaction server (authorization device), the location verification server including (Fig. 1 part 20): a location identification system for obtaining a location-related identifier associated with the source of the location verification request (column 5 lines 58-67); and a message constructor for encoding the location-related identifier into a message (column 5 lines 58-67); a transaction server (authorization device) adapted to receive the message, the transaction server including: a message decoder for decoding the location-related identifier encoded within the message (column 6 lines 1-15); and a transaction authorizer system for authorizing transaction between the user computer and the transaction processor if the pre-specified location comprises the location identified by the location-related identifier (column 6 lines 16-31); and a message

transmit facility for transporting the message from the location verification server (part 120) to the transaction server (part 20) (Fig. 1).

Although Rangedahl discloses the authentication information encoded into a message format (authorization request format), wherein the definition of encode is programming to put something into code, Rangedahl does not disclose encoding (encrypting) the location-related identifier into a message, thus the authentication information.

Stallings discloses a system for authentication wherein the user sends a ticket to the authentication server and the ticket includes that ID and network address of the user (page 328). The server provides the service (transaction) after the user is authenticated (Fig. 11.1).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the encryption of the system of Stalling to encrypt the authentication information in the system of Rangedahl. One of ordinary skill in the art would have been motivated to do this because encrypting the authentication information makes the system more secure so that eavesdroppers are discouraged from eavesdropping.

In reference to claim 9, Rangedahl discloses a system for remotely and automatically verifying the location of an electronic device and authorizing operation of the device if it resides in an allowed geographical location (abstract). Rangedahl discloses a verification server for receiving an incoming telephone call from a user desiring to conduct a location-dependent transaction with a transaction server, the verification server including (Fig. 2 in combination with column 3 lines 28-37): a decoder for obtaining a location-related identifier associated with the incoming telephone call (column 6 lines 1-15 in combination with column 4 lines 16-25); and location-related message constructor for encoding the location-related identifier into a location-

Art Unit: 2135

related message (column 5 lines 58-67); a transaction server adapted to receive the location-related message, the transaction server (authorization device) including (part 20 Fig. 2): a location-related message decoder for determining the location-related identifier encoded within the location-related message (column 6 lines 1-15); transaction authorization system for determining whether the pre-specified location comprises the location identified by the location-related identifier (column 6 lines 16-31); and a transaction processor for conducting the location-dependent transaction if the transaction authorization system determines the pre-specified location comprises the location identified by the location-related identifier (authorization device as in column 4 lines 1-15); and location-related message transmit facility transporting the location-related message from the verification server to the transaction server (column 4 line 65 to column 5 line 12).

Although Rangedahl discloses the authentication information encoded into a message format (authorization request format), wherein the definition of encode is programming to put something into code, Rangedahl does not disclose encoding (encrypting) the location-related identifier into a message, thus the authentication information.

Stallings discloses a system for authentication wherein the user sends a ticket to the authentication server and the ticket includes that ID and network address of the user (page 328). The server provides the service (transaction) after the user is authenticated (Fig. 11.1).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the encryption of the system of Stalling to encrypt the authentication information in the system of Rangedahl. One of ordinary skill in the art would have been

motivated to do this because encrypting the authentication information makes the system more secure so that eavesdroppers are discouraged from eavesdropping.

In reference to claim 10 Rangedahl discloses a system for remotely and automatically verifying the location of an electronic device and authorizing operation of the device if it resides in an allowed geographical location (abstract). Rangedahl discloses a location verification server for receiving a telephone call comprising a location verification request from a user computer desiring authorization to conduct a transaction with a transaction server, the location verification server including (column 4 lines 1-15): a location identification system for obtaining a location-related identifier associated with the user computer (column 4 lines 16-25); user identification system for obtaining a user identifier of the user associated with the location verification request (column 4 lines 16-25); and a message constructor for encoding the location-related identifier, the user identifier and the timestamp into a location verification message (column 5 lines 58-67); and a transaction authorization server adapted to process a location verification message, the transaction authorization server including: a message decoder for decoding the location-related identifier, the user identifier and the timestamp encoded within the location verification message (column 6 lines 1-15); and a transaction authorization system for authorizing a transaction for the user identified the user identifier if the pre-specified location comprises the location identified by the location-related identifier (column 6 lines 16-31); and a message transmit facility for transporting the message from the verification server to the transaction Server (part 120 and part 20 Fig. 1).

Although Rangedahl discloses the authentication information encoded into a message format (authorization request format), wherein the definition of encode is programming to put

something into code, Rangedahl does not disclose encoding (encrypting) the location-related identifier into a message, thus the authentication information.

Stallings discloses a system for authentication wherein the user sends a ticket to the authentication server and the ticket includes that ID and network address of the user (page 328). The server provides the service (transaction) after the user is authenticated (Fig. 11.1). Stallings further includes a clock capable of generating a timestamp associated with the location verification request (page 328 paragraph 2); and a transaction authorization system for authorizing a transaction for the user identified the user identifier if the pre-specified location comprises the location identified by the location-related identifier and the timestamp is less than a predetermined age (page 328 paragraph 2).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the encryption of the system of Stalling to encrypt the authentication information in the system of Rangedahl. One of ordinary skill in the art would have been motivated to do this because encrypting the authentication information makes the system more secure so that eavesdroppers are discouraged from eavesdropping.

In reference to claim 16, Rangedahl discloses a system for remotely and automatically verifying the location of an electronic device and authorizing operation of the device if it resides in an allowed geographical location (abstract). Rangedahl discloses a verification server for receiving an incoming telephone call from a user desiring to conduct a location-dependent transaction with a transaction server, the verification server including (Fig. 2 in combination with column 3 lines 28-37): a decoder for obtaining a location-related identifier associated with the incoming telephone call (column 6 lines 1-15 in combination with column 4 lines 16-25); and

Art Unit: 2135

location-related message constructor for encoding the location-related identifier into a location-related message (column 5 lines 58-67); a transaction server adapted to receive the location-related message, the transaction server (authorization device) including (part 20 Fig. 2): a location-related message decoder for determining the location-related identifier encoded within the location-related message (column 6 lines 1-15); transaction authorization system for determining whether the pre-specified location comprises the location identified by the location-related identifier (column 6 lines 16-31); and a transaction processor for conducting the location-dependent transaction if the transaction authorization system determines the pre-specified location comprises the location identified by the location-related identifier (authorization device as in column 4 lines 1-15); and location-related message transmit facility transporting the location-related message from the verification server to the transaction server (column 4 line 65 to column 5 line 12).

Although Rangedahl discloses the authentication information encoded into a message format (authorization request format), wherein the definition of encode is programming to put something into code, Rangedahl does not disclose encoding (encrypting) the location-related identifier into a message, thus the authentication information.

Stallings discloses a system for authentication wherein the user sends a ticket to the authentication server and the ticket includes that ID and network address of the user (page 328). The server provides the service (transaction) after the user is authenticated (Fig. 11.1). Stallings further includes a clock capable of generating a timestamp associated with the location verification request (page 328 paragraph 2); and a transaction authorization system for authorizing a transaction for the user identified the user identifier if the pre-specified location

comprises the location identified by the location-related identifier and the timestamp is less than a predetermined age (page 328 paragraph 2).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the encryption of the system of Stalling to encrypt the authentication information in the system of Rangedahl. One of ordinary skill in the art would have been motivated to do this because encrypting the authentication information makes the system more secure so that eavesdroppers are discouraged from eavesdropping.

In reference to claim 23, Rangedahl discloses a system for remotely and automatically verifying the location of an electronic device and authorizing operation of the device if it resides in an allowed geographical location (abstract). Rangedahl discloses a location verification server for receiving telephone call comprising a location verification request from a user computer desiring authorization to conduct transaction with a transaction server, the location verification server including (Fig 2 part 20): a location identification system for obtaining call identification information, the call identification information comprising information associated with the location of the call origin (column 4 lines 16-20); a location code generator for generating a location-related identifier based, at least in part, upon the call identification information (column 6 lines 1-15); a user identification system for obtaining a user identifier of the user associated with the location verification request (column 6 lines 16-30); and message constructor for encoding the location-related identifier, the user identifier, the message constructor being adapted to incorporate an message authentication sequence within the message (column 5 lines 58-67); message transmitter for transmitting the location verification message to the user computer (Fig. 3 B part 340); and a transaction authorization server adapted to process a location

verification message, the transaction authorization server including: a message receiver for receiving the location verification message from the user computer (part 120 Fig. 4); a message decoder for decoding the location-related identifier, the message decoder being adapted to reject the message if the message authentication sequence reflects that the message has been altered since had been encoded by the message constructor (column 4 lines 1-8).

Although Rangedahl discloses the authentication information encoded into a message format (authorization request format), wherein the definition of encode is programming to put something into code, Rangedahl does not disclose encoding (encrypting) the location-related identifier into a message, thus the authentication information.

Stallings discloses a system for authentication wherein the user sends a ticket to the authentication server and the ticket includes that ID and network address of the user (page 328). The server provides the service (transaction) after the user is authenticated (Fig. 11.1). Stallings further includes a clock capable of generating a timestamp associated with the location verification request (page 328 paragraph 2); and a transaction authorization system for authorizing a transaction for the user identified the user identifier if the pre-specified location comprises the location identified by the location-related identifier and the timestamp is less than a predetermined age (page 328 paragraph 2).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the encryption of the system of Stalling to encrypt the authentication information in the system of Rangedahl. One of ordinary skill in the art would have been motivated to do this because encrypting the authentication information makes the system more secure so that eavesdroppers are discouraged from eavesdropping.

In reference to claims 2, 11, and 17, wherein the location verification request from the user computer is made over a telephone network, and wherein the location-related identifier comprises at least a portion of the calling telephone number (Fig. 2 in combination with column 4 lines 16-25).

In reference to claims 3, 12, and 18, wherein the user computer is connected to the transaction server via a first network, and the message transmit facility transports the message to the transaction server over the telephone network, via the user computer, and over the first network (Fig. 2).

In reference to claims 4, 13, and 19, wherein the verification server is connected to the transaction server via a second network, and the message transmit facility is adapted to transport the message to the transaction server over the second network (Fig. 2).

In reference to claim 5, wherein the message-transmit facility is adapted to transmit the message to the transaction server while the user computer is connected to the verification server via the telephone network (Fig. 2).

In reference to claims 6, 14-15, and 20-21, wherein the message transmit facility is adapted to transmit a disconnect message to the transaction server when the user computer ceases to be connected to the verification server via the telephone network (Fig 3B part 350).

In reference to claim 7, wherein the location-related identifier comprises an indication of the user's longitude and latitude as determined by a transponder (column 5 lines 58-67).

In reference to claim 8, wherein the indication of the user's longitude and latitude is encrypted.

Although Rangedahl discloses the authentication information encoded into a message format (authorization request format), wherein the definition of encode is programming to put something into code, Rangedahl does not disclose encoding (encrypting) the location-related identifier into a message, thus the authentication information. The authentication information disclosed by Rangedahl includes longitude and latitude information (column 5 lines 58-67).

Stallings discloses a system for authentication wherein the user sends a ticket to the authentication server and the ticket includes that ID and network address of the user (page 328). The authentication information disclosed by Stallings is encrypted (page 328).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the encryption of the system of Stalling to encrypt the authentication information in the system of Rangedahl. One of ordinary skill in the art would have been motivated to do this because encrypting the authentication information makes the system more secure so that eavesdroppers are discouraged from eavesdropping.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paula W. Klimach whose telephone number is (571) 272-3854. The examiner can normally be reached on Mon to Thr 9:30 a.m to 5:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

PWK
Friday, September 30, 2005

JtS *S*
Primary Examiner
Art Unit 2135